1. **Conference**

|  |  |
| --- | --- |
| ارتفاع التعدين بيانات الأداء لكشف التسلل الشبكة | Research Title (Arabic) |
| High Performance Data Mining for Network Intrusion Detection | Research Title (English) |
| الحوسبة عالية الأداء ، واستخراج البيانات، | Research Topic (Arabic) |
| High performance computing, data mining, | Research Topic (English) |
| MIT | Publisher (Arabic) |
| MIT | Publisher (English) |
| 2004 | Publishing Year (Arabic) |
| 2004 | Publishing Year (English) |
| 0-88986-421-7 | ISBN |
| الكتلة الحوسبة، المعالجة المتوازية، واستخراج البيانات، كشف التسلل، وأمن الشبكات | Key Words (Arabic) |
| Cluster computing, parallel processing, data mining, intrusion detection, network security | Key Words (English ) |
| Parallel and Distributed Computing and Systems (PDCS 2004) | Journal Name, or (Conference + place and date being held) |
|  | Volume No. or Issue No. and the Number of Pages in case it has been published in a scientific journal |
| كمبيوتر كشف التسلل هو نهج لكشف الاختراقات يشتبه في أقرب وقت ممكن للحد من الأضرار التي لحقت النظام واتخاذ الإجراءات المناسبة باستخدام بيانات مراجعة الحسابات التي تم إنشاؤها بواسطة أجهزة الكمبيوتر. هناك نهجين أساسيين، الشاذة وكشف سوء الاستخدام. كشف شذوذ في تحديد السلوك الصحيح للنظام، ومن ثم الكشف عن السلوكيات الشاذة. الكشف عن سوء استخدام ليميز أنماط التدخل معروفة وتوليد قواعد صريحة لوصفها. ثم، وترصد لهذه الأنماط للإشارة إلى حدوث تسرب. ومع ذلك، هذه الخوارزميات هي مكلفة حسابيا ومراجعة البيانات وعادة ما تكون ضخمة جدا بحيث لا يمكن معالجتها يدويا أو البحث عن معلومات قيمة تجريبيا. نحن نستخدم تقنية عالية الأداء استخراج البيانات لاكتشاف المعرفة الخفية الكامنة وراء جزءا لا يتجزأ من كميات كبيرة من البيانات. نحن تطوير استخراج البيانات بالتوازي نموذجا لكشف التسلل باستخدام شبكة موازية backpropagation العصبية. نحن تقييم أداء نموذج المتقدمة من حيث تسريع، ومعدل التنبؤ، وكاذبة معدل الانذار. ونحن نقدم أيضا مكتبة البرمجة المتزامنة إننا نعمل على تطوير مكتبة دعا المرونة الحاسوبية (CRlib) لتنفيذ المقترح عالية خوارزميات التعدين بيانات الأداء | Research Abstract (Arabic) |
| Computer intrusion detection is an approach to detect suspected intrusions as soon as possible to reduce the damage to the system and take appropriate actions using the audit data generated by the computers. There are two basic approaches, anomaly detection and misuse detection. Anomaly detection is to define correct behavior of the system, and then to detect abnormal behaviors. Misuse detection is to characterize known intrusion patterns and generate explicit rules to describe them. Then, it monitors for those patterns to indicate an occurrence of intrusion. However, these algorithms are computationally expensive and the audit data are usually too huge to be processed manually or find valuable information heuristically. We use a high performance data mining technique to discover underlying hidden knowledge embedded in large volumes of data. We develop a parallel data mining model for intrusion detection using a parallel backpropagation neural network. We evaluate the performance of the developed model in terms of speedup, prediction rate, and false alarm rate. We also introduce the concurrent programming library we have been developing called Computational Resiliency library (CRlib) to implement the proposed high performance data mining algorithms. | Research Abstract (English) |